

CIRCULANT q -BUTSON HADAMARD MATRICES

TREVOR HYDE AND JOSEPH KRAISLER

ABSTRACT. If $q = p^n$ is a prime power, then a d -dimensional q -Butson Hadamard matrix H is a $d \times d$ matrix with all entries q th roots of unity such that $HH^* = dI_d$. We use algebraic number theory to prove a strong constraint on the dimension of a circulant q -Butson Hadamard matrix when $d = p^m$ and then explicitly construct a family of examples in all possible dimensions. These results relate to the long-standing circulant Hadamard matrix conjecture in combinatorics.

1. INTRODUCTION

For a prime power $q = p^n$, a q -Butson Hadamard matrix (q -BH) of dimension d is a $d \times d$ matrix H with all entries q th roots of unity such that

$$HH^* = dI_d,$$

where H^* is the conjugate transpose of H . A $d \times d$ matrix H is said to be *circulant* if

$$H_{ij} = f(i - j)$$

for some function f defined modulo d . In this paper we investigate circulant q -BH matrices of dimension $d = p^m$.

Theorem 1. *If $q = p^n$ is a prime power and $d = p^m$, then there exists a $d \times d$ circulant q -Butson Hadamard matrix if and only if $m \leq 2n$, with one exception when $(m, n, p) = (1, 1, 2)$.*

Our analysis of circulant q -BH matrices led us to the useful notion of *fibrous functions*.

Definition 2. *Let $d \geq 0$ and $q = p^n$ be a prime power,*

- (1) *If X is a finite set, we say a function $g : X \rightarrow \mathbb{Z}/(q)$ is **fibrous** if the cardinality of the fiber $|g^{-1}(b)|$ depends only on $b \bmod p^{n-1}$.*
- (2) *We say a function $f : \mathbb{Z}/(d) \rightarrow \mathbb{Z}/(q)$ is **δ -fibrous** if for each $k \not\equiv 0 \bmod d$ the function $\delta_k(x) = f(x + k) - f(x)$ is fibrous.*

When $q = d = p$ are both prime, δ -fibrous functions coincide with the concept of *planar functions*, which arise in the study of finite projective planes [2] and have applications in cryptography [6]. Circulant q -BH matrices of dimension d are equivalent to δ -fibrous functions $f : \mathbb{Z}/(d) \rightarrow \mathbb{Z}/(q)$.

Theorem 3. *Let $q = p^n$ be a prime power and ζ a primitive q th root of unity. There is a correspondence between $d \times d$ circulant q -Butson Hadamard matrices H and δ -fibrous functions $f : \mathbb{Z}/(d) \rightarrow \mathbb{Z}/(q)$ given by*

$$(H_{ij}) = (\zeta^{f(i-j)}).$$

We restate our main result in the language of δ -fibrous functions.

Date: March 14th, 2017.

Corollary 4. *If $q = p^n$ is a prime power, then there exist δ -fibrous functions $f : \mathbb{Z}/(p^m) \rightarrow \mathbb{Z}/(q)$ if and only if $m \leq 2n$ with one exception when $(m, n, p) = (1, 1, 2)$.*

It would be interesting to know if δ -fibrous functions have applications to finite geometry or cryptography.

When $q = 2$, q -BH matrices are called *Hadamard matrices*. Hadamard matrices are usually defined as $d \times d$ matrices H with all entries ± 1 such that $HH^t = dI_d$. Boston Hadamard matrices were introduced in [1] as a generalization of Hadamard matrices.

Circulant Hadamard matrices arise in the theory of difference sets, combinatorial designs, and synthetic geometry [7, Chap. 9]. There are arithmetic constraints on the possible dimension of a circulant Hadamard matrix. When the dimension $d = 2^m$ is a power of two we have:

Theorem 5 (Turyn [9]). *If $d = 2^m$ is the dimension of a circulant Hadamard matrix, then $m = 0$ or $m = 2$.*

Turyn's proof uses algebraic number theory, more specifically the fact that 2 is totally ramified in the 2^m th cyclotomic extension $\mathbb{Q}(\zeta_{2^m})/\mathbb{Q}$; an elementary exposition may be found in Stanley [8]. Conjecturally this accounts for all circulant Hadamard matrices [7].

Conjecture 6. *There are no d -dimensional circulant Hadamard matrices for $d > 4$.*

Circulant q -Butson Hadamard matrices provide a natural context within which to consider circulant Hadamard matrices. A better understanding of the former could lead to new insights on the latter. For example, our proof of Theorem 1 shows that the two possible dimensions for a circulant Hadamard matrix given by Turyn's theorem belong to larger family of circulant q -BH matrices with the omission of $d = 2$ being a degenerate exception. Circulant q -BH matrices have been studied in some specific dimensions [3], but overall seem poorly understood. We leave the existence of q -BH matrices when the dimension d is not a power of p for future work.

Acknowledgements. The authors thank Pdraig Cathain for pointers to the literature, in particular for bringing the work of de Launey [4] to our attention. We also thank Jeff Lagarias for helpful feedback on an earlier draft.

2. MAIN RESULTS

We always let $q = p^n$ denote a prime power. First recall the definitions of q -Butson Hadamard and circulant matrices.

Definition 7. *A d -dimensional q -Butson Hadamard matrix H (q -BH) is a $d \times d$ matrix all of whose entries are q th roots of unity satisfying*

$$HH^* = dI_d,$$

where H^ is the conjugate transpose of H .*

*A d -dimensional **circulant matrix** C is a $d \times d$ matrix with coefficients in a ring R such that*

$$C_{ij} = f(i - j)$$

for some function $f : \mathbb{Z}/(d) \rightarrow R$.

Example 8. Hadamard matrices are the special case of q -BH matrices with $q = 2$. The q -Fourier matrix (ζ^{ij}) where ζ is a primitive q th root of unity is an example of a q -BH matrix (which may

also be interpreted as the character table of the cyclic group $\mathbb{Z}/(q)$.) When $q = 3$ and ω is a primitive 3rd root of unity this is the matrix:

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega^4 \end{pmatrix}$$

This example is not a *circulant* 3-BH matrix. The following is a circulant 3-BH matrix:

$$\begin{pmatrix} 1 & \omega & \omega \\ \omega & 1 & \omega \\ \omega & \omega & 1 \end{pmatrix}$$

The remainder of the paper is divided into two sections: first we prove constraints on the dimension d of a circulant q -BH matrix when d is a power of p ; next we introduce the concept of δ -fibrous functions and construct examples of circulant q -BH matrices in all possible dimensions.

Constraints on dimension. Theorem 9 uses the ramification of the prime p in the q th cyclotomic extension $\mathbb{Q}(\zeta)/\mathbb{Q}$ to deduce strong constraints on the dimension of a q -BH matrix.

Theorem 9. *If $q = p^n$ is a prime power and H is a circulant q -Butson Hadamard matrix of dimension $d = p^{m+n}$, then $m \leq n$.*

Note that our indexing of m has changed from the introduction; this choice was made to improve notation in our proof. We use this indexing for the rest of the paper.

Proof of Theorem 9. Suppose $H = (a_{i-j})$ is a circulant q -Butson Hadamard matrix of dimension $d = p^{m+n}$. From H being q -BH of dimension d we have

$$HH^* = dI_d,$$

hence $\det(H) = \pm d^{d/2}$ and each eigenvalue α of H has absolute value $|\alpha| = \sqrt{d} = p^{(m+n)/2}$. On the other hand, since $H = (a_{i-j})$ is circulant, it has eigenvalues

$$\alpha_k = \sum_{j < d} a_j \zeta^{jk}. \quad (1)$$

for ζ a primitive d th root of unity with corresponding eigenvector

$$u_k^t = (1, \zeta^k, \zeta^{2k}, \dots, \zeta^{(d-1)k}).$$

These observations combine to give two ways of computing $\det(H)$.

$$\prod_k \alpha_k = \det(H) = \pm p^{(m+n)d/2}. \quad (2)$$

The identity (2) is the essential interaction between the circulant and q -BH conditions on H . The prime p is totally ramified in $\mathbb{Q}(\zeta)$, hence there is a unique prime ideal $\mathfrak{p} \subseteq \mathbb{Z}[\zeta]$ over $(p) \subseteq \mathbb{Z}$. Since all $\alpha_k \in \mathbb{Z}[\zeta]$, it follows from (2) that $(\alpha_k) = \mathfrak{p}^{v_k}$ as ideals of $\mathbb{Z}[\zeta]$ for some $v_k \geq 0$ and for each k . So either α_0/α_1 or α_1/α_0 is an element of $\mathbb{Z}[\zeta]$. Say α_0/α_1 is the integral quotient. We noted $|\alpha_k| = p^{(m+n)/2}$ for each k , hence $|\alpha_0/\alpha_1| = 1$. The only integral elements of $\mathbb{Z}[\zeta]$ with absolute value 1 are roots of unity, hence $\alpha_0/\alpha_1 = \pm \zeta^r$ for some $r \geq 0$, hence

$$\alpha_0 = \pm \zeta^r \alpha_1. \quad (3)$$

By (1) we have

$$\alpha_0 = \sum_{j < d} a_j \quad \alpha_1 = \sum_{j < d} a_j \zeta^j.$$

Each $j < d = p^{m+n}$ has a unique expression as $j = j_0 + j_1 p^m$ where $j_0 < p^m$ and $j_1 < p^n$. Let $\omega = \zeta^{p^m}$ be a primitive q th root of unity. Then

$$\zeta^j = \zeta^{j_0 + j_1 p^m} = \omega^{j_1} \zeta^{j_0}.$$

Writing α_1 in the linear basis $\{1, \zeta, \zeta^2, \dots, \zeta^{p^m-1}\}$ of $\mathbb{Q}(\zeta)/\mathbb{Q}(\omega)$ we have

$$\alpha_1 = \sum_{j < d} a_j \zeta^j = \sum_{j' < p^m} b_{j'} \zeta^{j'},$$

where $b_{j'}$ is a sum of p^n complex numbers each with absolute value 1. Now (3) says $\alpha_0 = \pm \omega^{j_0} \zeta^{-j_1} \alpha_1$ for some j_0 and j_1 , thus

$$\sum_{j < d} a_j = \alpha_0 = \pm \omega^{j_0} \zeta^{-j_1} \alpha_1 = \sum_{j' < p^m} \pm \omega^{j_0} b_{j'} \zeta^{j'-j_1}.$$

Comparing coefficients we conclude that

$$\alpha_0 = \pm \omega^{j_0} b_{j_1},$$

which is to say that α_0 is the sum of p^n complex numbers each with absolute value 1, hence $|\alpha_0| \leq p^n$. On the other hand we have $|\alpha_0| = p^{(m+n)/2}$. Thus $m + n \leq 2n \implies 0 \leq m \leq n$ as desired. \square

Remark. The main impediment to extending this result from $q = p^n$ to a general integer q is that we no longer have the total ramification of the primes dividing the determinant of H . It may be possible to get some constraint in certain cases from a closer analysis of the eigenvalues α_k and ramification, but we do not pursue this.

δ -Fibrous functions and construction of circulant q -BH matrices. Recall the notion of *fibrous functions* from the introduction:

Definition 10. Let $d \geq 0$ and $q = p^n$ be a prime power,

- (1) If X is a finite set, we say $g : X \rightarrow \mathbb{Z}/(q)$ is **fibrous** if the cardinality of the fibers $|g^{-1}(b)|$ depends only on $b \bmod p^{n-1}$.
- (2) We say a function $f : \mathbb{Z}/(d) \rightarrow \mathbb{Z}/(q)$ is **δ -fibrous** if for each $k \not\equiv 0 \bmod d$ the function $x \mapsto f(x+k) - f(x)$ is fibrous.

Lemma 11 is a combinatorial reinterpretation of the cyclotomic polynomials $\Phi_{p^n}(x)$.

Lemma 11. Let p be a prime and ζ a primitive p^n th root of unity.

- (1) If $\sum_{k < p^n} b_k \zeta^k = 0$ with $b_k \in \mathbb{Q}$, then b_k depends only on $k \bmod p^{n-1}$.
- (2) If X is a finite set and $g : X \rightarrow \mathbb{Z}/(p^n)$ is a function, then g is fibrous iff

$$\sum_{x \in X} \zeta^{g(x)} = 0.$$

Proof. (1) Suppose $\sum_{k < p^n} b_k \zeta^k = 0$ for some $b_k \in \mathbb{Q}$. Then $r(x) = \sum_{k < p^n} b_k x^k \in \mathbb{Q}[x]$ is a polynomial with degree $< p^n$ such that $r(\zeta) = 0$. So there is some $s(x) \in \mathbb{Q}[x]$ such that $r(x) = s(x) \Phi_{p^n}(x)$ where

$$\Phi_{p^n}(x) = \sum_{j < p} x^{jp^{n-1}}$$

is the p^n th cyclotomic polynomial—the minimal polynomial of ζ over \mathbb{Q} . Since $\deg \Phi_{p^n}(x) = p^n - p^{n-1}$, it follows that $\deg s(x) < p^{n-1}$. Let

$$s(x) = \sum_{i < p^{n-1}} a_i x^i$$

for some $a_i \in \mathbb{Q}$. Expanding $s(x)\Phi_{p^n}(x)$ we have

$$r(x) = s(x)\Phi_{p^n}(x) = \sum_{\substack{i < p^{n-1} \\ j < p}} a_i x^{i+jp^{n-1}}.$$

Comparing coefficients yields

$$b_k = b_{i+jp^{n-1}} = a_i,$$

which is to say, b_k depends only $i \equiv k \pmod{p^{n-1}}$.

(2) Suppose g is fibrous. For each $i < p^{n-1}$, let $a_i = |g^{-1}(i)|$. Then

$$\sum_{x \in X} \zeta^{g(x)} = \sum_{i < p^{n-1}} \sum_{j < p} a_i \zeta^{i+jp^{n-1}} = \Phi_{p^n}(\zeta) \sum_{i < p^{n-1}} a_i \zeta^i = 0.$$

Conversely, for each $k < p^n$ let $c_k = |g^{-1}(k)|$. Then

$$0 = \sum_{x \in X} \zeta^{g(x)} = \sum_{k < p^n} c_k \zeta^k,$$

and (1) implies c_k depends only on $k \pmod{p^{n-1}}$. Hence g is fibrous. \square

Theorem 12 establishes the equivalence between q -BH matrices of dimension d and δ -fibrous functions $f : \mathbb{Z}/(d) \rightarrow \mathbb{Z}/(q)$.

Theorem 12. *Let $q = p^n$ be a prime power. There is a correspondence between circulant q -Butson Hadamard matrices H of dimension d and δ -fibrous functions $f : \mathbb{Z}/(d) \rightarrow \mathbb{Z}/(q)$ given by*

$$(H_{i,j}) = (\zeta^{f(i-j)}).$$

Proof. Suppose f is δ -fibrous. Define the matrix $H = (H_{i,j})$ by $H_{i,j} = \zeta^{f(i-j)}$ where ζ is a primitive q th root of unity. H is plainly circulant and has all entries q th roots of unity. It remains to show that $HH^* = dI_d$, which is to say that the inner product $r_{j,j+k}$ of column j and column $j+k$ is 0 for each j and each $k \not\equiv 0 \pmod{d}$. For each $k \not\equiv 0 \pmod{d}$ the function $\delta_k(x) = f(x+k) - f(x)$ is fibrous. Then we compute

$$r_{j,j+k} = \sum_{i < d} \zeta^{f(i-j+k)-f(i-j)} = \sum_{i < d} \zeta^{\delta_k(i-j)} = 0,$$

where the last equality follows from Lemma 11 (2).

Conversely, suppose $H = (H_{i,j})$ is a circulant q -Butson Hadamard matrix. Then $H_{i,j} = \zeta^{f(i-j)}$ for some function $f : \mathbb{Z}/(d) \rightarrow \mathbb{Z}/(q)$. Since $HH^* = dI_d$ we have for each $k \not\equiv 0 \pmod{d}$,

$$0 = r_{j,j+k} = \sum_{i < d} \zeta^{f(i-j+k)-f(i-j)}.$$

Lemma 11 (2) then implies $\delta_k(x) = f(x+k) - f(x)$ is fibrous. Therefore f is δ -fibrous. \square

Lemma 13 checks that affine functions are fibrous. We use this in our proof of Theorem 14.

Lemma 13. *If $q = p^n$ is a prime power, then for all $a \not\equiv 0 \pmod q$ and arbitrary b , the function $f(x) = ax + b$ is fibrous.*

Proof. Since $a \not\equiv 0 \pmod q$,

$$\sum_{j < q} \zeta^{f(j)} = \sum_{j < q} \zeta^{aj+b} = \zeta^b \sum_{j < q} (\zeta^a)^j = 0.$$

Thus, by Lemma 11 (2) we conclude that f is fibrous. \square

Theorem 14. *If $q = p^n$ is a prime power, then there exists a circulant q -Butson Hadamard matrix of dimension $d = p^{m+n} = p^m q$ for each $m \leq n$ unless $(m, n, p) = (0, 1, 2)$.*

Our construction in the proof of Theorem 14 misses the family $(m, n, p) = (0, n, 2)$ for each $n \geq 1$. Lemma 15 records a quick observation that circumvents this issue for $n > 1$, as our construction does give circulant 2^{n-1} -BH matrices of dimension 2^n .

Lemma 15. *If $q = p^n$ is a prime power and there exists a circulant q -BH matrix of dimension d , then there exists a circulant $p^k q$ -BH matrix of dimension d for all $k \geq 0$.*

Proof. Every q th root of unity is also a $p^k q$ th root of unity, hence we may view a circulant q -BH matrix H of dimension d as a circulant $p^k q$ -BH for all $k \geq 0$. \square

Proof of Theorem 14. Our strategy is to first construct a sequence of functions

$$\delta_k : \mathbb{Z}/(p^m) \times \mathbb{Z}/(q) \rightarrow \mathbb{Z}/(q)$$

which are fibrous for each $k < p^m q$. If $i : \mathbb{Z}/(p^m) \times \mathbb{Z}/(q) \rightarrow \mathbb{Z}/(p^m q)$ is the bijection $i(x, y) = x + p^m y$, we define $f : \mathbb{Z}/(p^m q) \rightarrow \mathbb{Z}/(q)$ such that $f(z + k) - f(z) = \delta_k(x, y)$ when $z = i(x, y)$. Hence f is δ -fibrous and Theorem 12 implies the existence of a corresponding circulant q -BH matrix of dimension $p^m q$.

Now for each $k \geq 0$ define δ_k by

$$\delta_k(x, y) = ky + \sum_{j < k} S_j(x), \quad (4)$$

where

$$S_j(x) = \sum_{i < j} \chi(x + i), \quad \chi(x) = \begin{cases} 1 & x \equiv -1 \pmod{p^m}, \\ 0 & \text{otherwise.} \end{cases}$$

Observe that $S_j(x)$ counts the integers in the interval $[x, x + j)$ congruent to $-1 \pmod{p^m}$ (which only depends on $x \pmod{p^m}$.) Any interval of length $p^m j_1$ contains precisely j_1 integers congruent to $-1 \pmod{p^m}$. For each $j < p^m q$, write $j = j_0 + p^m j_1$ with $j_0 < p^m$ and $j_1 < q$, then

$$S_j(x) = \sum_{i < j_0 + p^m j_1} \chi(x + i) = \sum_{i < j_0} \chi(x + i) + j_1 = S_{j_0}(x) + j_1. \quad (5)$$

We show that δ_k is fibrous when $k < p^m q$. If $k \not\equiv 0 \pmod q$, then for each $x = x_0$ the function $\delta_k(x_0, y)$ is affine hence fibrous by Lemma 13. So $\delta_k(x, y)$ is fibrous. Now suppose $k = k'q$ for some $k' < p^m$. Using (5) we reduce (4) to

$$\delta_k(x, y) = \sum_{j < k'q} S_j(x) = \sum_{j_0 + p^m j_1 < k'q} S_{j_0}(x) + j_1 = \ell \sum_{j_0 < p^m} S_{j_0}(x) + p^m \binom{\ell}{2}, \quad (6)$$

where $k'q = p^m(k'p^{n-m}) = p^m\ell$. Here we use our assumption $m \leq n$. The definition of χ implies

$$S_{j_0}(x) = \begin{cases} 0 & j_0 < p^m - x \\ 1 & j_0 \geq p^m - x, \end{cases} \implies \sum_{j_0 < p^m} S_{j_0}(x) = x,$$

whence $\delta_k(x, y) = \ell x + p^m \binom{\ell}{2}$. Since $k' < p^m$ it follows that $\ell = k'p^{n-m} < p^n = q$, so $\delta_k(x, y)$ is affine hence fibrous by Lemma 13.

Define $f : \mathbb{Z}/(p^m q) \rightarrow \mathbb{Z}/(q)$ by $f(k) = \delta_k(0, 0)$. For this to be well-defined, it suffices to check that $\delta_{k+p^m q}(x, y) = \delta_k(x, y)$ with arbitrary k . By (4),

$$\begin{aligned} \delta_{k+p^m q}(x, y) &= (k + p^m q)y + \sum_{j < k+p^m q} S_j(x) \\ &= ky + \sum_{j < k} S_j(x) + \sum_{j < p^m q} S_{j+k}(x) \\ &= \delta_k(x, y) + \sum_{j < p^m q} S_{j+k}(x). \end{aligned}$$

The argument leading to (6) gives

$$\sum_{j < p^m q} S_{j+k}(x) = qx + p^m \binom{q}{2} = p^m \binom{q}{2}.$$

Finally, $p^m \binom{q}{2} \equiv 0 \pmod{q}$ unless $(m, n, p) = (0, n, 2)$. Lemma 15 implies that constructing an example for $(1, n-1, 2)$ implies the existence of example for $(0, n, 2)$, hence we proceed under the assumption that either $p \neq 2$ or $p = 2$ and $m > 0$. The case $(m, n, p) = (0, 1, 2)$ is an exception as one can check explicitly that there are no 2-dimensional Hadamard matrices. Hence it follows that f is well-defined. Let $i : \mathbb{Z}/(p^m) \times \mathbb{Z}/(q) \rightarrow \mathbb{Z}/(p^m q)$ be the bijection $i(x, y) = x + p^m y$. To finish the construction we suppose $z = i(x, y)$, show

$$f(z+k) - f(z) = \delta_k(x, y),$$

and then our proof that δ_k is fibrous for all $k < p^m q$ implies f is δ -fibrous. Theorem 12 translates this into the existence of a circulant q -BH matrix of dimension p^{m+n} . Now,

$$\begin{aligned} f(z+k) - f(z) &= \delta_{z+k}(0, 0) - \delta_z(0, 0) = \sum_{z \leq j < z+k} S_j(0) = \sum_{j-z < k} \sum_{i-z < j-z} \chi(i) \\ &= \sum_{j' < k} \sum_{i' < j'} \chi(x + i') = \sum_{j' < k} S_{j'}(x) = \delta_k(x, y). \end{aligned}$$

□

Remark. Padraig Cathain brought the work of de Launey [4] to our attention after reading an initial draft. There one finds a construction of circulant q -Butson Hadamard matrices of dimension q^2 for all prime powers q which appears to be closely related to our construction in Theorem 14.

Example 16. We provide two low dimensional examples to illustrate our construction. First we have an 8 dimensional circulant 4-BH matrix.

$$\begin{pmatrix} 1 & -1 & i & 1 & 1 & 1 & i & -1 \\ -1 & 1 & -1 & i & 1 & 1 & 1 & i \\ i & -1 & 1 & -1 & i & 1 & 1 & 1 \\ 1 & i & -1 & 1 & -1 & i & 1 & 1 \\ 1 & 1 & i & -1 & 1 & -1 & i & 1 \\ 1 & 1 & 1 & i & -1 & 1 & -1 & i \\ i & 1 & 1 & 1 & i & -1 & 1 & -1 \\ -1 & i & 1 & 1 & 1 & i & -1 & 1 \end{pmatrix}$$

Let ω be a primitive 3rd root of unity. The following is a 9 dimensional circulant 3-BH matrix.

$$\begin{pmatrix} 1 & \omega^2 & \omega & 1 & 1 & 1 & 1 & \omega & \omega^2 \\ \omega^2 & 1 & \omega^2 & \omega & 1 & 1 & 1 & 1 & \omega \\ \omega & \omega^2 & 1 & \omega^2 & \omega & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & 1 & \omega^2 & \omega & 1 & 1 & 1 \\ 1 & 1 & \omega & \omega^2 & 1 & \omega^2 & \omega & 1 & 1 \\ 1 & 1 & 1 & \omega & \omega^2 & 1 & \omega^2 & \omega & 1 \\ 1 & 1 & 1 & 1 & \omega & \omega^2 & 1 & \omega^2 & \omega \\ \omega & 1 & 1 & 1 & 1 & \omega & \omega^2 & 1 & \omega^2 \\ \omega^2 & \omega & 1 & 1 & 1 & 1 & \omega & \omega^2 & 1 \end{pmatrix}$$

Corollary 17 is an immediate consequence of our main results by Theorem 12.

Corollary 17. *If $q = p^n$ is a prime power and $d = p^{m+n}$, then there exists a δ -fibrous function $f : \mathbb{Z}/(p^{m+n}) \rightarrow \mathbb{Z}/(q)$ iff $m \leq n$, with the one exception of $(m, n, p) = (0, 1, 2)$.*

Closing remarks. Our analysis focused entirely on the existence of circulant p^n -BH matrices with dimension d a power of p . The number theoretic method of Theorem 9 cannot be immediately adapted to the case where d is not a power of p , although as we noted earlier, it may be possible to get some constraint with a closer analysis of the eigenvalues of a circulant matrix and the ramification over the primes dividing d in the d th cyclotomic extension $\mathbb{Q}(\zeta)/\mathbb{Q}$.

The family of examples constructed in Theorem 14 was found empirically. It would be interesting to know if the construction extends to any dimensions which are not powers of p .

REFERENCES

- [1] Butson, A.T. “Generalized Hadamard matrices” *Proc. Amer. Math. Soc.*, 13 (1962), pp. 894-898
- [2] Dembowski, Peter, and Theodore G. Ostrom. “Planes of order n with collineation groups of order n^2 .” *Mathematische Zeitschrift* 103.3 (1968): 239-258.
- [3] Hiranandani, Gaurush, and Jean-Marc Schlenker. “Small circulant complex Hadamard matrices of Butson type.” *European Journal of Combinatorics* 51 (2016): 306-314.
- [4] de Launey, Warwick. “Circulant $\text{GH}(p^2; \mathbb{Z}_p)$ exist for all primes p .” *Graphs Combin.* 8, no. 4, (1992): 317-321.
- [5] Leung, Ka Hin, and Bernhard Schmidt. “New restrictions on possible orders of circulant Hadamard matrices.” *Designs, Codes and Cryptography* 64.1 (2012): 143-151.
- [6] Nyberg, Kaisa, and Lars Ramkilde Knudsen. “Provable security against differential cryptanalysis.” *Annual International Cryptology Conference*. Springer Berlin Heidelberg, 1992.
- [7] Ryser, Herbert John. “Combinatorial mathematics.” Vol. 14. Washington, DC: Mathematical Association of America, 1963.
- [8] Stanley, Richard P. “Algebraic combinatorics.” *Springer* 20 (2013): 22.
- [9] Turyn, Richard. “Character sums and difference sets.” *Pacific Journal of Mathematics* 15.1 (1965): 319-346.

DEPT. OF MATHEMATICS, UNIVERSITY OF MICHIGAN, ANN ARBOR, MI 48109-1043,
E-mail address: tghyde@umich.edu

DEPT. OF MATHEMATICS, UNIVERSITY OF MICHIGAN, ANN ARBOR, MI 48109-1043,
E-mail address: jkrais@umich.edu